

The University of Chicago

THE INTEGRAL BASES
OF ALL QUARTIC FIELDS WITH A
GROUP OF ORDER EIGHT

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1934

By
ANTOINETTE MARIE KILLEN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

1936

The University of Chicago

THE INTEGRAL BASES
OF ALL QUARTIC FIELDS WITH A
GROUP OF ORDER EIGHT

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1934

By
ANTOINETTE MARIE KILLEN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

1936



TABLE OF CONTENTS

Section	Page
1. Introduction.....	1
2. Canonical form for the equation.....	2
3. Classification for fields having $\rho \equiv 2$ or 3 (mod 4).....	6
4. Classification for fields having $\rho \equiv 1$ (mod 4).....	7
5. Application of known theorems to the case of G_8 fields.....	10
6. Notation.....	11
7. Fields with ρ even.....	13
8. Fields with $\rho \equiv 3$ (mod 4).....	19
9. Fields with $\rho \equiv 1$ (mod 4).....	21
Vita.....	31



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548410_0032

THE INTEGRAL BASES OF ALL QUARTIC FIELDS
WITH A GROUP OF ORDER EIGHT

1. Introduction. It is well known¹ that in every algebraic field $R(\theta)$ of degree n there exist n linearly independent algebraic integers $\omega_1, \omega_2, \dots, \omega_n$ such that every integer α of the field is expressible in one and only one way in the form

$$\alpha = q_1\omega_1 + \dots + q_n\omega_n$$

where the q_i are rational integers. The ω 's are then said to form an integral basis of the field. The integral bases of all relative quadratic fields $K(\sqrt{\mu})$ where μ is in $K = R(\sqrt{m})$ have been found² by the theory of ideals, but these bases are given in terms of factorization of 2 and μ into prime ideals, the solution of a quadratic congruence modulo ideals, and further complicated processes. The integers of all normal quartic fields have been found by strictly elementary methods by A. A. Albert in his paper on "The integers of normal quartic fields", Annals of Mathematics, volume 31 (1930), pp. 381-418. By normal quartic fields is meant those algebraic fields formed by the adjunction to the field R of rational numbers of a root θ of a quartic equation with rational coefficients and either the cyclic group or the "Vierergruppe" with respect to R . Albert has obtained explicit formulae for the

¹Cf. L. E. Dickson, Algebren und ihre Zahlentheorie, p. 144

²Cf. J. Sommer, Vorlesungen über Zahlentheorie, Chapter V.

bases of the integers of such fields in terms of the coefficients of the corresponding quartic equation.

It is the purpose of this paper to accomplish for fields generated by a root ω of a quartic equation with rational coefficients and a Galois group of order eight with respect to R , what Albert has done for normal quartic fields. There are three such groups, each of which is derivable from either of the others by an interchange of the subscripts on the roots x_1, x_2, x_3, x_4 of the quartic equation. With this understanding we will discuss merely fields with the group

$$G_8 = \{I, (12), (34), (12)(34), (13)(24), (14)(23), (1423), (1324)\}.$$

Unlike the normal fields, the G_8 fields do not have the property that all the conjugate fields coincide with the original field. This fact leads to the principal difference in the methods used in this paper and in that of Albert.

The early part of the paper is devoted to a discussion of a canonical form for the equations, a classification of equations into types giving non-equivalent sets of fields, and to the application of known theorems to the case of the fields under discussion. The remainder of the paper is concerned with the setting up and solution of the congruences which lead to the formulae for the bases.

2. Canonical form for the equation. It is known¹ that by a Tschirnhausen transformation

$$\xi = \eta_1 \omega^3 + \eta_2 \omega^2 + \eta_3 \omega + \eta_4, \quad (\eta_1, \dots, \eta_4 \text{ in } R),$$

¹R. Garver, "Quartic equations with certain groups", Annals of Mathematics, volume 29 (1928).

the equation

$$(1) \quad \Phi(\omega) \equiv \omega^4 + \xi_1 \omega^3 + \xi_2 \omega^2 + \xi_3 \omega + \xi_4 = 0, \quad (\xi_1, \dots, \xi_4 \text{ in } R),$$

whose group with respect to R is G_8 may be reduced to the form

$$(2) \quad \Psi(\zeta) \equiv \zeta^4 - 2g\zeta^2 + g^2 - f^2\rho = 0, \quad (\rho, f, \text{ and } g \text{ in } R),$$

where none of ρ , $g^2 - f^2\rho$, $\rho(g^2 - f^2\rho)$ may be the square of a rational number and ρ has no square factor $\neq 1$.

Conversely if

$$(3) \quad \rho \neq \delta_i^2, \quad g^2 - f^2\rho \neq \delta_i^2, \quad \rho(g^2 - f^2\rho) \neq \delta_i^2$$

[for any δ_i ($i = 1, 2, 3$) in R] , then (2) has the group G_8 with respect to R . Thus if $\Phi(x) = 0$, then $\Psi(y) = 0$, where

$$y = \eta_1 x^3 + \eta_2 x^2 + \eta_3 x + \eta_4$$

is in $R(x)$ and $R(y) = R(x)$, so that we have

THEOREM 1. Let the group of (1) be G_8 . Then if $\Phi(x) = 0$ the field $R(x)$ contains a primitive¹ quantity y satisfying (2) with (3) holding. Conversely, let y satisfy (2) with (3) holding. Then the group of $\Psi(\zeta)$ with respect to R is G_8 and the field $R(y)$ is a quartic field with group G_8 .

Consider now the equation (2). Suppose $g = c_1/c_2$, $f^2\rho = b_1/b_2$, where the c 's and b 's are rational integers and the fractions are in lowest terms, and let $\Psi(y) = 0$ and write $i = c_2 b_2 y$. Then $R(y) = R(i)$, where i satisfies

$$(4) \quad i^4 - 2c_1 c_2 b_2^2 i^2 + c_1^2 c_2^2 b_2^4 - c_2^4 b_1 b_2^3 = 0.$$

¹I.e., a quantity y in $R(x)$ such that $R(y) = R(x)$.

Clearly (4) is of essentially the same form as (2) with a relation corresponding to (3) holding among the coefficients. We may return then to our original notation used in (2), with the understanding that now the coefficients are integers. Moreover, we may assume that g and f have no square factor different from 1 in common, for if they had such a factor ν^2 then, writing $g = \nu^2 g_0$, $f = \nu^2 f_0$ we would have

$$\mathcal{P}(\zeta) = \zeta^4 - 2g_0\nu^2\zeta^2 + \nu^4(g_0^2 - f_0^2\rho)$$

and clearly i/ν would satisfy (2) with f and g replaced by f_0 and g_0 .

We now adopt the notation

$$i^2 = g + fu,$$

$$u^2 = \rho$$

and see that $1, u, i, ui$ form a basis of the quantities of $R(i)$.

In order to avoid in the work which follows the unnecessary handling of special cases to which equivalent fields give rise, we discuss at this point the transforming of the generator of the field $R(i)$ by means of the transformation

$$i_0 = i(\alpha_1 + \alpha_2 u).$$

Evidently $R(i) = R(i_0)$, since $R(i_0)$ contains i_0^2 and hence u , and thus contains $i_0/(\alpha_1 + \alpha_2 u)$. In fact the only proper subfields of a G_8 field $R(i)$ are R and $R(u)$ while i_0 is not in $R(u)$ by its form and hence is primitive. It is also true conversely that if $R(i) = R(i_0)$, two fields with the subfield $u^2 = \rho$, and i^2 and i_0^2 are in $R(u)$, then necessarily $i_0 = i(\alpha_1 + \alpha_2 u)$, where α_1 and α_2 are rational numbers. For since i_0 is in $R(i)$ we may write $i_0 = a_1 + a_2 i$, [a_1 and a_2 in $R(u)$], and therefore

$$i_0^2 = a_1 + 2a_1a_2i + a_2^2(g + fu).$$

Hence $a_1a_2 = 0$, since i_0^2 is in $R(u)$. But clearly $a_2 \neq 0$. Hence $i_0 = a_2i$.

The transformation then is in effect

$$(5) \quad \begin{aligned} g_0 &= (\alpha_1^2 + \alpha_2^2 \rho)g + 2\alpha_1\alpha_2 f\rho, \\ f_0 &= (\alpha_1^2 + \alpha_2^2 \rho)f + 2\alpha_1\alpha_2 g. \end{aligned}$$

As we have indicated above, we will always wish to employ rational integer f_0 and g_0 without common square factors. Consequently we will use only transformations having α and α_2 rational integers and we understand that any common square factors of g_0 and f_0 so obtained are to be divided out by a transformation $i_0 = \alpha^2 i$.

We will indicate the transformation which insures¹

$(g_0, f_0, \rho) = 1$. Let $(g, f, \rho) = p$ and write $g = pg_1$, $f = pf_1$, $\rho = p\rho_1$. Then let $\alpha_1 = p$ and let $\alpha_2 = 1$. We obtain

$$\begin{aligned} g_0 &= g_{01}/p^2 = (p + \rho_1)g_1 + 2f_1\rho_1, \\ f_0 &= f_{01}/p^2 = (p + \rho_1)f_1 + 2g_1 \end{aligned}$$

Suppose $(g_0, f_0, \rho) = p_1$. Then $(p + \rho_1)g_1 \equiv (p + \rho_1)f_1 + 2g_1 \equiv 0 \pmod{p_1}$. If a factor of p_1 does not divide $(p + \rho_1)$ it divides g_1 and hence f_1 . Since $(g_1, f_1, \rho_1) = 1$ such a factor divides p . But this is impossible since f and g had no common square factors, and hence $(p + \rho_1) \equiv 0 \pmod{p_1}$. Hence $p(p + \rho_1) = p^2 + \rho \equiv 0 \pmod{p_1}$ and hence p_1 divides both p and ρ . Hence $p_1 = 1$, since ρ had no square factors other than 1.

Having secured the result $(g_0, f_0, \rho) = 1$ we shall avoid

¹We shall use throughout the paper the notation $(a, b, c) = d$ to mean that d is the greatest common divisor of a , b , and c .

any transformation having $(\alpha, \rho) = p$, $p \neq 1$, since after such a transformation evidently $(g_0, f_0, \rho) \equiv 0 \pmod{p}$.

It is of course clear that the transformation (5) leaves ρ invariant and hence fields having different ρ 's are not equivalent. However, each of the cases $\rho \equiv 1, 2$, or $3 \pmod{4}$ decomposes into sub-cases, many of which can be shown to be equivalent. In the next two sections we shall make a classification of fields having $\rho \equiv 1, 2$, or 3 into non-equivalent types.

3. Classification for fields having $\rho \equiv 2$ or $3 \pmod{4}$.

In the first case, $\rho \equiv 2 \pmod{4}$, which we shall consider in Section 7, the possible cases (1) f odd, (2) $f \equiv 2$, $g \equiv 1$ or $3 \pmod{4}$, and (3) $f \equiv 0$, $g \equiv 1$ or $3 \pmod{4}$, arise. As indicated above, nothing is gained by a transformation having $\alpha_1 \equiv 0 \pmod{2}$ for which $(\alpha, \rho) = 2p_2$, or by a transformation having $(\alpha, \alpha_2) = 2p_0$, since common factors 4 are to be divided out. Furthermore the transformation $\alpha_1 \equiv 1$, $\alpha_2 \equiv 0 \pmod{2}$ gives the results $g_0 \equiv g$, $f_0 \equiv f \pmod{4}$. The only transformations which serve to eliminate any of the above cases are then those having $\alpha_1 \equiv \alpha_2 \equiv 1 \pmod{2}$. By means of such transformations

$f \equiv 1 \pmod{2}$ is transformed into $f_0 \equiv 1 \pmod{2}$,
 $f \equiv 2, g \equiv 3 \pmod{4}$ is transformed into $f_0 \equiv 0, g_0 \equiv 1 \pmod{4}$,
 $f \equiv 0, g \equiv 3 \pmod{4}$ is transformed into $f_0 \equiv 2, g_0 \equiv 1 \pmod{4}$

and conversely. Thus only the cases on the right need be considered and by considering all possible types of transformations we have shown that none of those cases can be eliminated. We may then state

THEOREM 2. Every G_8 field with $\rho \equiv 2 \pmod{4}$ is equivalent to such a field with $f \equiv 1 \pmod{2}$, $f \equiv 0, g \equiv 1 \pmod{4}$, or $f \equiv 2, g \equiv 1 \pmod{4}$.

In the case $\rho \equiv 3 \pmod{4}$ we have in addition to the sub-cases (1) - (3) above, the cases (4) $f \equiv g \equiv 2 \pmod{4}$, (5) $g \equiv 2$, $f \equiv 0 \pmod{4}$, and (6) $g \equiv 0$, $f \equiv 2 \pmod{4}$. Using a transformation with $\alpha_1 \equiv 1$, $\alpha_2 \equiv 0 \pmod{2}$ we obtain $g_0 \equiv g$, $f_0 \equiv f \pmod{4}$ and using $\alpha_1 \equiv 0$, $\alpha_2 \equiv 1 \pmod{2}$ we obtain $g_0 \equiv \rho g$, $f_0 \equiv \rho f \pmod{4}$. Hence by the latter transformation

$f \equiv 1 \pmod{2}$ is transformed into $f_0 \equiv 1 \pmod{2}$,
 $f \equiv 2 \pmod{4}$ is transformed into $f_0 \equiv 2 \pmod{4}$,
 $f \equiv 0$, $g \equiv 3 \pmod{4}$ is transformed into $f_0 \equiv 0$, $g_0 \equiv 1 \pmod{4}$,

and conversely.

By the transformation $\alpha_1 \equiv \alpha_2 \equiv 1 \pmod{2}$

$g \equiv f \equiv 2 \pmod{4}$ is transformed into $g_0 \equiv f_0 \equiv 1 \pmod{2}$,
 $g \equiv 2$, $f \equiv 0 \pmod{4}$ is transformed into $g_0 \equiv 0$, $f_0 \equiv 1 \pmod{2}$,
 $g \equiv 0$, $f \equiv 2 \pmod{4}$ is transformed into $g_0 \equiv 1$, $f_0 \equiv 0 \pmod{2}$,

and conversely. Hence we have

THEOREM 3. Every G_8 field with $\rho \equiv 3 \pmod{4}$ is equivalent to such a field with f odd, $f \equiv 2 \pmod{4}$, $g \equiv 1 \pmod{2}$, or $f \equiv 0$, $g \equiv 1 \pmod{4}$.

4. Classification for fields having $\rho \equiv 1 \pmod{4}$. This case is far more complicated than the cases of Section 3, and a more lengthy discussion is required not only for the question of equivalence of fields, but also for the solution of the congruences to which the non-equivalent fields give rise. In seeking to eliminate cases it is evident that the transformations $\alpha_1 \equiv 0$, $\alpha_2 \equiv 1$ and $\alpha_1 \equiv 1$, $\alpha_2 \equiv 0 \pmod{2}$ are not in general effective since they transform f and g into $f_0 \equiv f$ and $g_0 \equiv g \pmod{4}$, and as we shall need to observe later, into $f_0 \equiv f$, $g_0 \equiv g \pmod{8}$ for f and g even. By means of the transformation

$$\alpha_i \equiv \alpha_2 \equiv 1 \pmod{2}$$

$$(6) \quad \begin{aligned} g \equiv 0, f \equiv 2 \pmod{4} & \text{ is transformed into } g_0 \equiv f_0 \equiv 1 \pmod{2}, \\ g \equiv 2, f \equiv 0 \pmod{4} & \text{ is transformed into } g_0 \equiv f_0 \equiv 1 \pmod{2}, \\ g \equiv 1, f \equiv 0 \pmod{2} & \text{ is transformed into } g_0 \equiv f_0 \equiv 2 \pmod{4}, \\ g \equiv 0, f \equiv 1 \pmod{2} & \text{ is transformed into } g_0 \equiv f_0 \equiv 2 \pmod{4}. \end{aligned}$$

It is not true conversely that $g_0 \equiv f_0 \equiv 1 \pmod{2}$ or $g_0 \equiv f_0 \equiv 2 \pmod{4}$ can be transformed into the cases on the left in (6), as can be demonstrated in the example $g = 1, f = 3, \rho = 17$. We call attention to the fact also that if $g^2 - f^2\rho = s^2\sigma$, σ having no square factor > 1 , then σ is invariant under this transformation.

If σ is even then $g \equiv f \equiv 1 \pmod{2}$ may be transformed into $g_0 \equiv f_0 \equiv 2 \pmod{4}$ in the following way: let $\alpha_i = g$, $\alpha_2 = -f$; then

$$(7) \quad \begin{aligned} g_0 &= g(g^2 + f^2\rho - 2f^2\rho) = g(g^2 - f^2\rho) = gs^2\sigma, \\ f_0 &= f(g^2 + f^2\rho - 2g^2) = -f(g^2 - f^2\rho) = -fs^2\sigma, \end{aligned}$$

and the same transformation carries $f \equiv g \equiv 2 \pmod{4}$ into $f_0 \equiv g_0 \equiv 1 \pmod{2}$. If, however, g and f are odd and σ is odd, then g and f cannot be transformed into the case $g_0 \equiv f_0 \equiv 2 \pmod{4}$. For if g is odd then $g_0g \equiv 2 \pmod{4}$ implies $(g_0g)g \equiv g_0 \equiv 2 \pmod{4}$ and conversely. But

$$\begin{aligned} g_0g &= (\alpha_1^2 + \alpha_2^2\rho)g^2 + 2\alpha_1\alpha_2fg\rho \\ &= (\alpha_1g + \alpha_2f\rho)^2 + \alpha_2^2\rho(g^2 - f^2\rho) \\ &= (\alpha_1g + \alpha_2f\rho)^2 + \alpha_2^2\rho s^2\sigma. \end{aligned}$$

Likewise

$$\begin{aligned} f_0f &= (\alpha_1^2 + \alpha_2^2\rho)f^2 + 2\alpha_1\alpha_2gf \\ &= (\alpha_1f + \alpha_2g)^2 - \alpha_2^2(g^2 - f^2\rho) \end{aligned}$$

$$= (\alpha_1 f + \alpha_2 g)^2 - \alpha_2^2 s^2 \sigma.$$

Since a square is congruent to 0 or 1 (mod 4) it is clear that after all possible common factors four are removed from g_0 and f_0 the resulting $g_{01}g$ and $f_{01}f$ will have the form

$$g_{01}g \equiv (1 \text{ or } 0) + s_0^2 \sigma \pmod{4},$$

$$f_{01}f \equiv (1 \text{ or } 0) - s_0^2 \sigma \pmod{4}.$$

If $\sigma \equiv 1 \pmod{4}$, then $f_{01}f$ cannot be congruent to 2 (mod 4);

if $\sigma \equiv 3 \pmod{4}$, then $g_{01}g$ cannot be congruent to 2 (mod 4).

Conversely it is true that if σ is odd then $g \equiv f \equiv 2 \pmod{4}$ cannot be transformed into g and f both odd.

If $\sigma \equiv 1 \pmod{4}$, then by the transformation (7) $f \equiv 2 \pmod{8}$ may be transformed into $f_0 \equiv 6 \pmod{8}$. But this is not possible for $\sigma \equiv 3 \pmod{4}$ as can be seen from consideration of the general transformation

$$g_0 \equiv g_0(g')^2 \equiv 2g' [(\alpha_1 g' + \alpha_2 f' \rho)^2 + \alpha_2^2 \rho (s')^2 \sigma] \pmod{8},$$

$$f_0 \equiv f_0(f')^2 \equiv 2f' [(\alpha_1 f' + \alpha_2 g' \rho)^2 - \alpha_2^2 (s')^2 \sigma] \pmod{8}$$

on any case for which $(s')^2 = s^2/4 \not\equiv 0 \pmod{16}$, as for example for $f' = f/2 = 1$, $g' = g/2 = 7$, $\rho = 5$, in which case $\sigma = 11 \equiv 3 \pmod{4}$.

Furthermore it can readily be seen that $f \equiv 2 \pmod{8}$ cannot be transformed into $f \equiv 6 \pmod{8}$ for all even σ .

Finally, in the case $f \equiv g \equiv 2 \pmod{4}$, σ odd, we wish to insure $\alpha_1 > 4$. This may be accomplished by a transformation having α_1 odd and prime to ρ and α_2 even, by which transformation $f_0 \equiv f \pmod{8}$, $g_0 \equiv g \pmod{8}$. For we have then

$$g_0^2 - f_0^2 \rho = (g^2 - f^2 \rho)(\alpha_1^2 - 4\rho)^2$$

and it is sufficient to show that $\alpha_1^2 - 4\rho$, which is odd for α odd, contains a factor which does not divide g_0 . In other words, we wish to choose α , odd so that

$$\frac{g_0}{\alpha_1^2 - 4\rho} = \frac{(\alpha^2 + 4\rho)g + 4\alpha f\rho}{\alpha_1^2 - 4\rho} = g + \frac{4\rho(\alpha f + 2g)}{\alpha^2 - 4\rho}$$

is not an integer. This is possible since

$$|\alpha^2 - 4\rho| > |\alpha(4\rho f)| + |8g\rho|$$

for α , sufficiently large.

The results of this Section may be summarized in

THEOREM 5. Every G_8 field with $\rho \equiv 1 \pmod{4}$ is equivalent to such a field with (1) $g \equiv f \equiv 1 \pmod{2}$, σ odd; (2) $g \equiv f \equiv 2 \pmod{4}$, σ even; (3) $f \equiv 2 \pmod{8}$, $g \equiv 2 \pmod{4}$, $\sigma \equiv 1 \pmod{4}$, $\alpha_2 > 4$; or (4) $g \equiv f \equiv 2 \pmod{4}$, $\sigma \equiv 3 \pmod{4}$, $\alpha_2 > 4$.

5. Application of known¹ theorems to the case of G_8 fields. Let $1, -1, j, -j$ be the roots of $\Psi(\zeta) = 0$ and define $\bar{a}(1) = a(-1)$. Then employing the argument used in Albert's "Integers of normal quartic fields" it can be shown that

LEMMA 1. If a is an integer of $R(1)$ then $\bar{a}$ is also such an integer.

LEMMA 2. Every quartic field generated by a quantity 1 satisfying a quartic equation with group G_8 contains a quadratic sub-field $R(u)$, $u^2 = \rho$, where $\rho \neq 1$ has no square factor. Any such sub-field has as a basis of its integers the basis $1, P$ where $P = u$ if $\rho \equiv 2, 3 \pmod{4}$ and $2P = u + 1$, $P^2 = P + n$ if $\rho = 4n + 1$.

¹Dickson, Algebren und ihre Zahlentheorie, Chapter 8.

THEOREM 6. The integers of any quartic field $R(i)$ having the group G_8 are exclusively those quantities a given by

$$a = a_1 + a_2 i \quad [a_1 \text{ and } a_2 \text{ in } R(u)] ,$$

such that

$$a + \bar{a}, \quad a\bar{a}$$

are integers of $R(u)$.

In accordance with the notation agreed upon $\bar{a} = a_1 - a_2 i$,
 $a + \bar{a} = 2a_1$, $a\bar{a} = a_1^2 - a_2^2 i^2$. Hence we have

THEOREM 7. The integers

$$a = a_1 + a_2 i \quad [a_1 \text{ and } a_2 \text{ in } R(u)]$$

of a quartic field having the group G_8 are exclusively those quantities a for which

$$2a_1, \quad a_1^2 - a_2^2 i^2$$

are integers of $R(u)$.

It is true that the integers are necessarily those for which $2a_2 i^2$ is an integer of $R(u)$, but this fact was not found to be of material assistance.

6. Notation. For the convenience of the reader we insert here the notation which we shall adopt in the following pages. We let τ be the greatest common divisor of f and g , and write $f = \tau f_1$, $g = \tau g_1$. Then if t and r are the greatest common divisors of f_1, τ and g_1, τ respectively we may write $f_1 = t f_2$, $g_1 = r g_2$, and $\tau = r t \tau'$ since of course τ has no square factor. Furthermore $g^2 - f^2 \rho = \tau^2 (g_1^2 - f_1^2 \rho)$. We write $g_1^2 - f_1^2 \rho = \sigma_2^2 \sigma_1$, where $\sigma_1 \neq 1$ has no square factors $\neq 1$, and define $\sigma = \tau \sigma_2$. Hence $g^2 - f^2 \rho = \tau^2 \sigma_2^2 \sigma_1 = \sigma^2 \sigma_1$. We let d be the

greatest common divisor of σ_1 and τ and write $\sigma_1 = d\sigma_2$,

$\tau_1 = d\tau_2$. Finally we write $w = (-f\rho g_1^{\phi-1} + u)/d\sigma_2$, $m = (g_1^\phi - 1)/d\sigma_2$, where ϕ is the Euler ϕ -function for $d\sigma_2$ so that $g_1^\phi \equiv 1 \pmod{d\sigma_2}$ and hence m is an integer.

The w so defined will appear in the bases we are seeking and is readily shown to be an algebraic integer. For we make use of the fact contained in Theorem 6 that w is an integer if and only if $w + \bar{w}$ and $w\bar{w}$ are integers of $R(u)$. Clearly $w + \bar{w} = 0$. Computing $w\bar{w} = w^2$ we have

$$\begin{aligned} w^2 &= \frac{(-f_1\rho g_1^{\phi-1} + u)^2(g + fu)}{d^2\sigma_2^2} \\ &= \frac{rt\tau_2(g_1f_1^2\rho^2g_1^{2\phi-2} + g_1\rho - 2f_1^2\rho^2g_1^{\phi-1})}{d\sigma_2^2} \\ &\quad + \frac{rt\tau_2(f_1^3\rho^2g_1^{2\phi-2} + f_1\rho - 2f_1g_1\rho g_1^{\phi-1})u}{d\sigma_2^2} \end{aligned}$$

To show that the term free from u is an ordinary integer we multiply the numerator by g_1 , which is prime to $d\sigma_2$. The new numerator is then

$$rt\tau_2(f_1^2\rho^2g_1^{2\phi} + g_1^2\rho - 2f_1^2\rho^2g_1^\phi)$$

Hence, substituting $g_1^\phi = 1 + md\sigma_2$ and neglecting the factor $rt\tau_2$ this becomes

$$\begin{aligned} &f_1^2\rho^2(1 + 2md\sigma_2 + m^2d^2\sigma_2^2) + g_1^2\rho - 2f_1^2\rho^2(1 + md\sigma_2) \\ &= \rho(g_1^2 - f_1^2\rho) + m^2d^2\sigma_2^2f_1^2\rho^2 \\ &= \rho\sigma_2^2d\sigma_3 + m^2d^2\sigma_2^2f_1^2\rho^2 \end{aligned}$$

which is clearly divisible by $d\sigma_2$. To show that the coefficient of u is an integer we multiply by g_1^2 and obtain for the numerator neglecting the factor $rt\tau_2$,

$$\begin{aligned} & f_1(f_1^2 \rho^2 g_1^2 \phi + g_1^2 \rho - 2g_1^2 \rho g_1^2 \phi) \\ &= f_1[f_1^2 \rho^2 (1+2md\sigma_2 + m^2 d^2 \sigma_2^2) + g_1^2 \rho - 2g_1^2 \rho (1+md\sigma_2)] \\ &= f_1[\rho(f_1^2 \rho - g_1^2) + 2md\sigma_2 \rho(f_1^2 \rho - g_1^2) + f_1^2 \rho^2 m^2 d^2 \sigma_2^2] \\ &\equiv 0 \pmod{d\sigma_2^2} \end{aligned}$$

since $f_1^2 \rho - g_1^2 = \sigma_2^2 \sigma_1 \equiv 0 \pmod{d\sigma_2^2}$.

7. Fields with ρ even. By Theorem 7 the quantity $2a_1$ is an integer of $R(u)$ and we may write $a_1 = \beta/2 + (\rho/2)u$, where β , and ρ are rational integers. Write

$$a_2 = \frac{\delta_1}{u_1 u_0} + \frac{\delta_2}{u_2 u_0} u = \frac{1}{u_1 u_2 u_0} (\delta_1 u_2 + \delta_2 u_1 u)$$

where the Greek letters are rational integers, $(\delta_1, u_1 u_0) = 1$,

$(\delta_2, u_1 u_0) = 1$, and $(u_1 u_0, u_2 u_0) = u_0$. The quantity

$$a_1^2 - a_2^2 u^2 = \frac{(\beta^2 + 2\beta\rho u + \rho^2 u^2)}{4} - \frac{(\delta_1^2 u_2^2 + 2u_1 u_2 \delta_1 \delta_2 u + u_1^2 \delta_2^2 \rho^2)(g + fu)}{u_0^2 u_1^2 u_2^2}$$

is an integer of $R(u)$ and hence

$$(8) \quad (\beta_1^2 + \beta_2^2 \rho) u_0^2 u_1^2 u_2^2 - 4g(\delta_1^2 u_2^2 + u_1^2 \delta_2^2 \rho) - 8f u_1 u_2 \delta_1 \delta_2 \rho \equiv 0 \pmod{4u_0^2 u_1^2 u_2^2}$$

$$(9) \quad \beta_1 \beta_2 u_0^2 u_1^2 u_2^2 - 4g(\delta_1 \delta_2 u_1 u_2) - 2f(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho) \equiv 0 \pmod{2u_0^2 u_1^2 u_2^2}$$

Let $u_i = 2v_1$ or v_1 according as $u_i \equiv 0$ or $1 \pmod{2}$; that is, let

$$u_1 = 2^{\mu_1} v_1, \quad \mu_1 = 0 \text{ or } 1,$$

$$u_2 = 2^{\mu_2} v_2, \quad \mu_2 = 0 \text{ or } 1.$$

Then from (9) $-2f\delta_2^2 u_1^2 \equiv 0 \pmod{2^{\mu_1} v_1}$ and hence $f \equiv 0 \pmod{v_1}$,

since u_2 and δ_1 are prime to u_1 . Hence from (8) $4g\delta_1^2 u_2^2 \equiv 0$

$\pmod{2^{2\mu_1} v_1^2}$ and therefore $g \equiv 0 \pmod{v_1^2}$. Hence from (9) $f \equiv 0$

$\pmod{v_1^2}$ and therefore $v_1 = 1$, since f and g have no common square factor other than 1.

From (9) $-2f\delta_2^2 u_1^2 \equiv 0 \pmod{2^{\mu_2} v_2}$ and therefore $f \equiv 0$

(mod v_2). Hence from (8) $-4g v_1^2 \delta_2^2 \rho \equiv 0 \pmod{2^{2\mu_2} v_2^2}$ and therefore $g\rho \equiv 0 \pmod{v_2^2}$. Since ρ has no square factor, $g \equiv 0 \pmod{v_2}$, whence from (9) $f\rho \equiv 0 \pmod{v_2^2}$ and therefore $f \equiv g \equiv \rho \equiv 0 \pmod{v_2}$ and hence $v_2 = 1$.

Multiplying (8) by $-f$, (9) by $2g$, dropping 4 from the modulus, and reducing modulo $v_1^2 v_1' v_2^2$ we have

$$\begin{aligned} 4fg\delta_1^2 v_2^2 + 4fg\delta_2^2 v_1^2 \rho + 8f^2 \delta_1 \delta_2 v_1 v_2 \rho &\equiv 0 \pmod{v_1^2 v_1' v_2^2}, \\ -4fg\delta_1^2 v_2^2 - 4fg\delta_2^2 v_1^2 \rho - 8g^2 \delta_1 \delta_2 v_1 v_2 &\equiv 0 \pmod{v_1^2 v_1' v_2^2} \end{aligned}$$

and hence adding we have

$$8\delta_1 \delta_2 v_1 v_2 (f^2 \rho - g^2) \equiv 0 \pmod{v_1^2 v_1' v_2^2}.$$

Case I. If either v_1 or $v_2 \equiv 0 \pmod{2}$, we have $4(f^2 \rho - g^2) \equiv 0 \pmod{v_1^2}$.

Case II. If neither v_1 nor $v_2 \equiv 0 \pmod{2}$, we have $8(f^2 \rho - g^2) \equiv 0 \pmod{v_1^2}$.

Hence if we let $g^2 - f^2 \rho = \sigma^2 \sigma$, where σ has no square factor, then $v_1 v_2$ and $v_2 v_1$ divide 4σ . Hence we may write

$$a = a_1 + a_2 i = \frac{(\beta_1 + \beta_2 u)}{2} + \frac{(\gamma_1 + \gamma_2 u)i}{4\sigma},$$

where again the Greek letters represent rational integers but where we no longer assume the fractions are in lowest terms. We may then replace (8) and (9) by

$$(10) \quad 4(\beta_1^2 + \beta_2^2 \rho) \sigma^2 - g(\gamma_1^2 + \gamma_2^2 \rho) - 2f\rho \gamma_1 \gamma_2 \equiv 0 \pmod{16\sigma^2},$$

$$(11) \quad 8\beta_1 \beta_2 \sigma^2 - f(\gamma_1^2 + \gamma_2^2 \rho) - 2g \gamma_1 \gamma_2 \equiv 0 \pmod{16\sigma^2}.$$

Then we have, using $\sigma^2 = \tau^2 \sigma_2^2$, $\tau = (f, g)$,

$$(12) \quad 4(\beta_1^2 + \beta_2^2 \rho) \tau \sigma_2^2 - g_1(\gamma_1^2 + \gamma_2^2 \rho) - 2f_1 \rho \gamma_1 \gamma_2 \equiv 0 \pmod{16\tau \sigma_2^2},$$

$$(13) \quad 8\beta_1 \beta_2 \tau \sigma_2^2 - f_1(\gamma_1^2 + \gamma_2^2 \rho) - 2g_1 \gamma_1 \gamma_2 \equiv 0 \pmod{16\tau \sigma_2^2}.$$

We next make use of $(g_1, \tau) = r$, $(f_1, \tau) = t$, $\tau = rt\tau$ and observe that rt is prime to ρ and, since ρ is even, prime to 2. From (12) and (13) we obtain

$$(14) \quad rg_2(\gamma_1^2 + \gamma_2^2 \rho) + 2tf_2\rho\gamma_1\gamma_2 \equiv 0 \pmod{rt\tau\sigma_2^2},$$

$$(15) \quad tf_2(\gamma_1^2 + \gamma_2^2 \rho) + 2rg_2\gamma_1\gamma_2 \equiv 0 \pmod{rt\tau\sigma_2^2}$$

and therefore $2tf_2\rho\gamma_1\gamma_2 \equiv 0 \pmod{r}$. But $2tf_2\rho$ is prime to r , so that $\gamma_1\gamma_2 \equiv 0 \pmod{r}$, and from (15) $\gamma_1 \equiv \gamma_2 \equiv 0 \pmod{r}$. Similarly $\gamma_1 \equiv \gamma_2 \equiv 0 \pmod{t}$.

Write

$$(16) \quad \gamma_1 = rt\gamma_3, \quad \gamma_2 = rt\gamma_4.$$

Then we have

$$(17) \quad g_1(\gamma_3^2 + \gamma_4^2 \rho) + 2f_1\rho\gamma_3\gamma_4 \equiv 0 \pmod{\tau\sigma_2^2},$$

$$(18) \quad f_1(\gamma_3^2 + \gamma_4^2 \rho) + 2g_1\gamma_3\gamma_4 \equiv 0 \pmod{\tau\sigma_2^2}.$$

Now g_1 is prime to $\tau\sigma_2^2$. Hence (17) is equivalent to

$$(19) \quad g_1^2(\gamma_3^2 + \gamma_4^2 \rho) + 2g_1f_1\rho\gamma_3\gamma_4 \equiv 0 \pmod{\tau\sigma_2^2}$$

which may be written

$$(20) \quad \begin{aligned} &g_1^2\gamma_3^2 + 2g_1f_1\rho\gamma_3\gamma_4 + f_1^2\rho^2\gamma_4^2 + (g_1^2 - f_1^2\rho)\rho\gamma_4^2 \equiv 0 \pmod{\tau\sigma_2^2}, \\ &(g_1\gamma_3 + f_1\rho\gamma_4)^2 + \sigma_2^2\tau\rho\gamma_4^2 \equiv 0 \pmod{\tau\sigma_2^2}. \end{aligned}$$

Hence, dropping τ from the modulus and reducing modulo σ_2^2 we have $(g_1\gamma_3 + f_1\rho\gamma_4)^2 \equiv 0 \pmod{\sigma_2^2}$ and therefore

$$(g_1\gamma_3 + f_1\rho\gamma_4) \equiv 0 \pmod{\sigma_2}.$$

Let

$$g_1\gamma_3 = -f_1\rho\gamma_4 + h\sigma_2.$$

Then from (20) we obtain

$$(21) \quad h^2 \sigma_2^2 + \sigma_2 \sigma_2^2 \rho \chi_4^2 \equiv 0 \pmod{\tau \sigma_2^2}.$$

Finally using $(\tau, \sigma) = d$ we see from (21) that $h = dh_1$. Multiplying (17) by f_1 and (18) by g_1 and subtracting we have

$$2 \chi_3 \chi_4 (f_1^2 \rho - g_1^2) = -2 \chi_3 \chi_4 \sigma_2^2 \sigma_1 \equiv 0 \pmod{\tau \sigma_2^2};$$

therefore $\chi_3 \chi_4 \equiv 0 \pmod{\tau_2}$ since in this case 2 is prime to τ_2 . Therefore from (19) $\chi_3 \equiv 0$, $\chi_4 \equiv 0 \pmod{\tau_2}$; that is, we may write

$$(22) \quad \chi_3 = \tau_2 \chi_5, \quad \chi_4 = \tau_2 \chi_6$$

and from (21) $h_1 \equiv 0 \pmod{\tau_2}$. Thus we have shown in view of § 6, (16), and (22) that the integers $\underline{a}$ of Theorem 2 have the form

$$\begin{aligned} \underline{a} &= \frac{\beta}{2} + \frac{\beta_2 u}{2} + \left(\frac{\chi_1}{4\sigma} + \frac{\chi_2 u}{4\sigma} \right) i = \frac{\beta}{2} + \frac{\beta_2 u}{2} + \left(\frac{rt \tau_2 \chi_5}{4rt \tau_2 d \sigma_2} + \frac{rt \tau_2 \chi_6 u}{4rt \tau_2 d \sigma_2} \right) i \\ &= \frac{\beta}{2} + \frac{\beta_2 u}{2} + \frac{(\chi_5 + \chi_6 u)}{4 d \sigma_2} i, \end{aligned}$$

where, if ϕ is the Euler ϕ -function for $d \sigma_2$, then

$$\chi_5 \equiv -f_1 \rho g_1^{\phi-1} \chi_6 \pmod{d \sigma_2}.$$

We have then

$$a_1^2 - a_2^2 i^2 = \frac{1}{4} (\beta_1^2 + 2\beta_1 \beta_2 u + \beta_2^2 \rho) - \frac{1}{16 d^2 \sigma_2^2} (\chi_5^2 + 2\chi_5 \chi_6 u + \chi_6^2 \rho) (g + fu)$$

and hence

$$(23) \quad 4(\beta_1^2 + \beta_2^2 \rho) d^2 \sigma_2^2 - g(\chi_5^2 + \rho \chi_6^2) - 2f \rho \chi_5 \chi_6 \equiv 0 \pmod{16 d^2 \sigma_2^2},$$

$$(24) \quad 8\beta_1 \beta_2 d^2 \sigma_2^2 - f(\chi_5^2 + \rho \chi_6^2) - 2g \chi_5 \chi_6 \equiv 0 \pmod{16 d^2 \sigma_2^2}.$$

It remains to solve the congruences modulo 16. From Theorem 2 it is clear that we need only consider bases for the three cases f odd, $f \equiv 2$, $g \equiv 1$, and $f \equiv 0$, $g \equiv 1 \pmod{4}$ and understand that in the other cases we are to transform the generating element of the field so as to obtain such integral f

and g .

Case I. f odd. From (24), since $\rho \equiv 2 \pmod{4}$, we have $\gamma_5 \equiv 0 \pmod{2}$ and hence $\gamma_6 \equiv 0 \pmod{2}$. Hence we may let $\gamma_5 = 2\gamma_7$, $\gamma_6 = 2\gamma_8$ and, since $d\alpha_2 \equiv 1 \pmod{2}$,

$$(25) \quad (\beta_1^2 + 2\beta_2^2) - g(\gamma_7^2 + 2\gamma_8^2) \equiv 0 \pmod{4},$$

$$(26) \quad 2\beta_1\beta_2 - f(\gamma_7^2 + 2\gamma_8^2) - 2g\gamma_7\gamma_8 \equiv 0 \pmod{4}$$

Again from (26) $\gamma_7 \equiv 0 \pmod{2}$ and hence $\gamma_8 \equiv \beta_1\beta_2 \pmod{2}$. But from (25) $\beta_1 \equiv 0 \pmod{2}$ and therefore $\gamma_7 \equiv \gamma_8 \equiv \beta_1 \equiv \beta_2 \equiv 0 \pmod{2}$.

Case II. $f \equiv 2$, $g \equiv 1 \pmod{4}$. From (23) $\gamma_5 \equiv 0 \pmod{2}$ and hence $\gamma_6 \equiv 0 \pmod{2}$. Whence from (25) $\beta_1 \equiv \gamma_7 \pmod{2}$. Hence we have

$$(\gamma_7^2 + 2\beta_2^2) - (\gamma_7^2 + 2\gamma_8^2) \equiv 0 \pmod{4},$$

$$2\beta_2\gamma_7 - 2\gamma_7^2 - 2\gamma_7\gamma_8 \equiv 0 \pmod{4},$$

and hence $\beta_2^2 - \gamma_8^2 \equiv 0 \pmod{2}$, and hence the possible solutions are

$$\beta_1 \equiv \beta_2 \equiv \gamma_7 \equiv \gamma_8 \equiv 0 \pmod{2}, \quad \beta_1 \equiv \gamma_7 \equiv 0, \quad \beta_2 \equiv \gamma_8 \equiv 1 \pmod{2}.$$

Case III. $f \equiv 0$, $g \equiv 1 \pmod{4}$. As before $\gamma_5 \equiv \gamma_6 \equiv 0 \pmod{2}$ implies $\beta_1 \equiv \gamma_7 \pmod{2}$. Hence we have

$$\beta_2^2 - \gamma_8^2 \equiv 0 \pmod{2},$$

$$\gamma_7(\beta_2 - \gamma_8) \equiv 0 \pmod{2}.$$

Hence the possible solutions are

$$\beta_1 \equiv \gamma_7 \equiv 0 \pmod{2}, \quad \beta_2 \equiv \gamma_8 \equiv 0 \text{ or } 1 \pmod{2},$$

$$\beta_1 \equiv \gamma_7 \equiv 1 \pmod{2}, \quad \beta_2 \equiv \gamma_8 \equiv 0 \text{ or } 1 \pmod{2}.$$

We may now say that our integers have the form

$$a = \frac{\beta_1}{2} + \frac{\beta_2}{2}u + \left(\frac{\gamma_7}{2d\alpha_2} + \frac{\gamma_8}{2d\alpha_2}u \right)1.$$

Moreover

$$2\gamma_1 \equiv -f_1 \rho g_1^{\phi^{-1}} \cdot 2\gamma_0 \pmod{d\sigma_2}.$$

Now 2 is prime to $d\sigma_2$ and hence

$$\gamma_1 \equiv -f_1 \rho g_1^{\phi^{-1}} \gamma_0 \pmod{d\sigma_2}.$$

Write

$$\gamma_1 = -f_1 \rho g_1^{\phi^{-1}} \gamma_0 + \lambda d\sigma_2.$$

Then substituting we have

$$a = \frac{\beta_1}{2} + \frac{\beta_2}{2} u + \frac{(-f_1 \rho g_1^{\phi^{-1}} \gamma_0 + \lambda d\sigma_2) i}{2 d\sigma_2} + \frac{\gamma_0 u i}{2 d\sigma_2}$$

or we may write

$$a = \frac{\beta_1}{2} + \frac{\beta_2 u}{2} + \frac{\lambda i}{2} + \frac{\gamma_0 w}{2}$$

where w was defined in §6 and $\gamma_1 \equiv \lambda \pmod{2}$.

The solutions of the congruences for the three cases show that in the first case the integers have the form

$$I = \beta_3 + \beta_4 u + \lambda_1 i + \gamma_0 w;$$

in the second case they have the forms I and

$$I_1 = \beta_3 + \frac{\beta_2}{2} u + \lambda_1 i + \frac{\gamma_0}{2} w;$$

and in the third case they have the forms I , I_1 ,

$$I_2 = \frac{\beta_1}{2} + \beta_4 u + \frac{\lambda}{2} i + \gamma_0 w, \quad I_3 = \frac{\beta_1}{2} + \frac{\beta_2}{2} u + \frac{\lambda}{2} i + \frac{\gamma_0}{2} w,$$

where the Greek letters represent rational integers and $\beta_1, \beta_2, \lambda, \gamma_0$ are odd. Hence for the first case $1, u, i, w$ form a basis for the integers of $R(1)$. For the second case $1, u, i, (u+w)/2$ form such a basis, and for the third case $1, u, (i+1)/2, (u+w)/2$ form a basis.

For the first case the statement is obvious. For the second case we must first show that $(u+w)/2$ is an algebraic integer, which can be done in a manner similar to that used in proving that w itself is an integer in Section 6. Next we observe that we may express any integer I as an integral combination of $1, u, 1, (u+w)/2$ by writing

$$I = \beta_3 + (\beta_4 - \gamma_6)u + \lambda_1 + 2\gamma_6 \frac{(u+w)}{2}$$

To express an integer I_1 as an integral combination of these basal quantities write

$$I_1 = \beta_3 + \frac{(\beta_4 - \gamma_6)}{2} u + \lambda_1 + \gamma_6 \frac{(u+w)}{2}.$$

Since β_4 and γ_6 are odd $(\beta_4 - \gamma_6)/2$ is a rational integer. A similar argument applies to the third case. Hence we may state

THEOREM 8. Let f, g, ρ be the integer parameters of the general G_8 quartic in its canonical form (2) where $\rho, g^2 - f^2\rho$, and $\rho(g^2 - f^2\rho)$ are not the squares of rational numbers. Then if 1 satisfies (2), $R(1)$ contains a quadratic subfield $R(u), u^2 = \rho$, where $\rho \neq 1$ has no square factor. If $\rho \equiv 2 \pmod{4}$ and w is defined as in §6, the values of the parameters which give rise to non-equivalent fields $R(1)$ are (1) f odd, in which case $1, u, 1, w$ form a basis for the integers of $R(1)$, (2) $f \equiv 2, g \equiv 1 \pmod{4}$, in which case $1, u, 1, (u+w)/2$ form such a basis, and (3) $f \equiv 0, g \equiv 1 \pmod{4}$ where $1, u, (1+1)/2, (u+w)/2$ form a basis

3. Fields with $\rho \equiv 3 \pmod{4}$. By Lemma 2 the basis for the integers of $R(u)$ is $1, u$ in this case also. Referring to Theorem 3 we note that the cases which it will be necessary for us to consider all have τ odd, and hence it is easily verified that the reduction for the part of the modulus not containing 2

explicitly in the case ρ even carries over without change to this case, since the only place where explicit use was made of the fact $\rho \equiv 0 \pmod{2}$ was in proving rt and τ prime to 2, which is clearly true for the cases under consideration. Hence we have again the results stated in § 7 below equation (22).

Case I. $f \equiv 1 \pmod{2}$. We recall therefore (23) and (24). Clearly from (24) $\gamma_5 \equiv \gamma_6 \pmod{2}$ and since $\rho \equiv 3 \pmod{4}$ it follows readily from (23) that $\gamma_5 \gamma_6 \equiv 0 \pmod{2}$. Hence $\gamma_5 \equiv \gamma_6 \equiv 0 \pmod{2}$ and we have

$$(27) \quad (\beta_1^2 + 3\beta_2^2) - g(\gamma_7^2 + 3\gamma_8^2) - 2\gamma_7\gamma_8 \equiv 0 \pmod{4},$$

$$(28) \quad 2\beta_1\beta_2 - f(\gamma_7^2 + 3\gamma_8^2) - 2g\gamma_7\gamma_8 \equiv 0 \pmod{4}.$$

From (28) $\gamma_7 \equiv \gamma_8 \pmod{2}$, hence from (27) $\beta_1 \equiv \beta_2 \pmod{2}$, hence $\gamma_7\gamma_8 \equiv 0 \pmod{2}$, and hence $\gamma_7 \equiv \gamma_8 \equiv 0 \pmod{2}$ from (27), whence from (28) $\beta_1 \equiv \beta_2 \equiv 0 \pmod{2}$. Hence in this case our integers have the form I of § 7, where w and λ are defined as before.

Case II. $g \equiv 1, f \equiv 0 \pmod{2}$. If now we apply first (23) and then (24) we again obtain $\gamma_5 \equiv \gamma_6 \equiv 0 \pmod{2}$ and reduce our congruences to

$$(\beta_1^2 + 3\beta_2^2) - g(\gamma_7^2 + 3\gamma_8^2) \equiv 0 \pmod{4},$$

$$2\beta_1\beta_2 - f(\gamma_7^2 + 3\gamma_8^2) - 2g\gamma_7\gamma_8 \equiv 0 \pmod{4}.$$

If $f \equiv 2 \pmod{4}$ the solutions are evidently $\beta_1 \equiv \beta_2 \equiv \gamma_7 \equiv \gamma_8 \equiv 0$ or $1 \pmod{2}$ and the integers are of the forms I and I_3 of § 7, where $\lambda \equiv \gamma_7 \pmod{2}$ because f_1 is even and $d\alpha_2$ is odd.

If $f \equiv 0 \pmod{4}$ the solutions are

$$\beta_1 \equiv \beta_2 \equiv \gamma_7 \equiv \gamma_8 \equiv 0 \text{ or } 1 \pmod{2},$$

$$\beta_1 \equiv \gamma_7 \equiv 0, \quad \beta_2 \equiv \gamma_8 \equiv 1 \pmod{2},$$

$$\beta_1 \equiv \gamma_7 \equiv 1, \quad \beta_2 \equiv \gamma_8 \equiv 0 \pmod{2}.$$

In this case the integers have the form I, I_1, I_2 , or I_3 . An argument similar to that at the end of § 7 results in the following

THEOREM 9. Let $R(1)$ be a G_8 field of Theorem 8 with $\rho \equiv 3 \pmod{4}$. Then the values of the parameters which give rise to non-equivalent fields are (1) f odd, in which case $1, u, 1, w$ form a basis for the integers of $R(1)$, (2) $g \equiv 1 \pmod{2}$, $f \equiv 2 \pmod{4}$, in which case $1, u, 1, (1+u+1+w)/2$ form a basis, and (3) $g \equiv 1, f \equiv 0 \pmod{4}$, in which case $1, u, (1+1)/2, (u+w)/2$ form a basis.

9. Fields with $\rho \equiv 1 \pmod{4}$. Since by Lemma 2 the basis for the integers of $R(u)$ is $1, P$ where $P = (u+1)/2$, $P^2 = n+P$ if $\rho = 4n + 1$, we cannot refer at once to our earlier results but must make a development similar to that of Section 7. It turns out to be advantageous to let

$$2a_1 = \beta_1 + \beta_2 P, \quad a_2 = \frac{\delta_1}{u_1 u_0} + \frac{\delta_2}{u_2 u_0} u = \frac{1}{u_1 u_2 u_0} (\delta_1 u_2 + \delta_2 u_1 u),$$

where the Greek letters are defined as in the first paragraph of § 7. We again use the fact that $a_1^2 - a_2^2 1^2$ is an integer of $R(u)$. We have

$$\begin{aligned} a_1^2 - a_2^2 1^2 &= \frac{1}{4} [\beta_1^2 + 2\beta_1 \beta_2 P + \beta_2^2 (P+n)] - \frac{1}{u_1^2 u_2^2 u_0^2} (\delta_1^2 u_2^2 + 2\delta_1 \delta_2 u_1 u_2 + \delta_2^2 u_1^2 \rho) (g + fu) \\ &= \frac{1}{4} [\beta_1^2 + 2\beta_1 \beta_2 P + \beta_2^2 (P+n)] - \frac{1}{u_1^2 u_2^2 u_0^2} [g(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho) + 2f\rho\delta_1 \delta_2 u_1 u_2 + f(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho)u + 2g\delta_1 \delta_2 u_1 u] \\ &= \frac{1}{4} [\beta_1^2 + \beta_2^2 n + (2\beta_1 \beta_2 + \beta_2^2)P] - \frac{1}{u_1^2 u_2^2 u_0^2} [(g-f)(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho) + 2(f\rho - g)\delta_1 \delta_2 u_1 u_2 \\ &\quad + 2f(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho)P + 4g\delta_1 \delta_2 u_1 u_2 P], \end{aligned}$$

from which we derive the congruences

$$(29) \quad (\beta_1^2 + \beta_2^2 n) u_1^2 u_2^2 - 4(g-f)(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho) - 8(f\rho - g)\delta_1 \delta_2 u_1 u_2 \equiv 0 \pmod{4 u_1^2 u_2^2 u_0^2},$$

$$(30) \quad (2\beta_1 \beta_2 + \beta_2^2) u_1^2 u_2^2 - 6f(\delta_1^2 u_2^2 + \delta_2^2 u_1^2 \rho) - 16g\delta_1 \delta_2 u_1 u_2 \equiv 0 \pmod{4 u_1^2 u_2^2 u_0^2}.$$

Let

$$v_1 = 2^{\mu_1} v_1, \quad \mu_1 = 0, 1, 2,$$

$$v_2 = 2^{\mu_2} v_2, \quad \mu_2 = 0, 1, 2.$$

Then from (30) v_1 divides $8f$ and hence $2v_1$ divides $4f$. From (29) v_1 divides $4(g-f)$ and hence $2v_1$ divides $4g$. Hence v_1^2 divides $8f$ and $4(g-f)$ and hence v_1^2 divides f and g and hence $v_1 = 1$. Consider now with (30) the congruence (29.1) obtained by multiplying (29) by 2 and adding to (30). Thus

$$(29.1) \quad (2\beta_1^2 + 2\beta_2^2 n + 2\beta_1\beta_2 + \beta_2^2 v_2^2 v_0^2 - 8g(\delta_1^2 v_2^2 + \delta_2^2 v_1^2 \rho) - 16f\rho\delta_1\delta_2 v_1 v_2 \equiv 0 \pmod{v_1^2 v_2^2 v_0^2},$$

$$(30) \quad (2\beta_1\beta_2 + \beta_2^2) v_1^2 v_2^2 - 8f(\delta_1^2 v_2^2 + \delta_2^2 v_1^2 \rho) - 16g\delta_1\delta_2 v_1 v_2 \equiv 0 \pmod{v_1^2 v_2^2 v_0^2}.$$

Then from (30) v_2 divides $8f\rho$ and hence from (29.1) v_2^2 divides $8g\rho$ and hence v_2^2 divides $g\rho$. But ρ has no square factor so v_2 must divide g and hence from (30) v_2^2 divides $f\rho$ and hence v_2 divides f . Since f and g have no square factor in common, v_2 must divide ρ also and hence $v_2 = 1$. But $(v_1, v_2) = 1$ so that either $v_1 = 1$ or $v_2 = 1$.

Finally let us neglect the first terms in (29.1) and (30), multiply (29.1) by f and (30) by g and subtract, obtaining

$$16(g^2 - f^2\rho) \delta_1\delta_2 v_1 v_2 \equiv 0 \pmod{v_1^2 v_2^2 v_0^2}.$$

Case I. If either v_1 or v_2 is divisible by 4 we have $4(g^2 - f^2\rho) \equiv 0 \pmod{v_0^2}$ and hence v_0 divides 2σ .

Case II. If neither v_1 nor v_2 is divisible by 4 we have $16(g^2 - f^2\rho) \equiv 0 \pmod{v_0^2}$ and hence v_0 divides 4σ .

In either case $v_1 v_0$ and $v_2 v_0$ divide 8σ and hence we may write

$$a = a_1 + a_2 i = \frac{\beta_1}{2} + \frac{\beta_2}{2} P + \left(\frac{\gamma_1}{8\sigma} + \frac{\gamma_2}{8\sigma} u \right) i,$$

where again the Greek letters represent rational integers but

where we no longer assume the fractions are in lowest terms.

In fact we have written $\chi_i/8\sigma = \delta_i/\nu_i \nu_6$ ($i = 1, 2$). We have shown that in either case $4\sigma = \nu_6 h$, where h is a rational integer, and hence $\chi_i \nu_i = 2\delta_i h$. Since either ν_i or ν_6 is equal to 1, the corresponding χ_i must be even.

We recall now the results of Theorem 5 and note that the cases giving rise to independent fields are $g \equiv f \equiv 1 \pmod{2}$ with σ_1 odd; $g \equiv f \equiv 2 \pmod{4}$ with σ_1 even; $f \equiv 2 \pmod{8}$, $g \equiv 2 \pmod{4}$ with $\sigma_1 \equiv 1 \pmod{4}$; and $g \equiv f \equiv 2 \pmod{4}$ with $\sigma_1 \equiv 3 \pmod{4}$. Furthermore in the last two cases we may assume that $\sigma_2 > 4$.

We may replace (29) and (30) by

$$\begin{aligned} (\beta_1^2 + \beta_2^2 n)16\sigma^2 - (g-f)(\chi_1^2 + \rho\chi_2^2) - 2(f\rho - g)\chi_1\chi_2 &\equiv 0 \pmod{64\sigma^2}, \\ (2\beta_1\beta_2 + \beta_2^2)8\sigma^2 - f(\chi_1^2 + \rho\chi_2^2) - 2g\chi_1\chi_2 &\equiv 0 \pmod{32\sigma^2} \end{aligned}$$

In order to solve these congruences with respect to the literal part of the modulus we shall consider the congruences

$$\begin{aligned} g(\chi_1^2 + \rho\chi_2^2) + 2f\rho\chi_1\chi_2 &\equiv 0 \pmod{\sigma^2}, \\ f(\chi_1^2 + \rho\chi_2^2) + 2g\chi_1\chi_2 &\equiv 0 \pmod{\sigma^2}. \end{aligned}$$

Clearly the cases which we are to consider have $f_1 \equiv g_1 \equiv 1 \pmod{2}$ in which cases $rt \equiv 1 \pmod{2}$. The reduction therefore is again the same as in the case $\rho \equiv 2 \pmod{4}$ up to and including equation (21), after which point a slight change in the argument is necessary in case $\tau_2 \equiv 0 \pmod{2}$. We make use of the fact observed above that either χ_1 or χ_2 is even. Hence, since $rt \equiv 1 \pmod{2}$ either χ_3 or χ_4 is even and hence, since $\tau \not\equiv 0 \pmod{4}$, we have again $\chi_3\chi_4 \equiv 0 \pmod{\tau_2}$. The remainder of the argument is the same.

Hence the integers are of the form

$$a = \frac{\beta_1}{2} + \frac{\beta_2}{2}P + \left(\frac{\gamma_5}{8d\sigma_2} + \frac{\gamma_4u}{8d\sigma_2}\right)i, \quad \gamma_5 \equiv -f_1\rho g_1^{\phi-1}\chi \pmod{d\sigma_2}$$

Clearly σ_2 is even for $g_1 \equiv f_1 \equiv 1 \pmod{2}$, and in this case d may be even. It appears therefore to be advantageous to substitute for γ_5 and thus remove $d\sigma_2$ from the modulus before solving our congruences modulo 2. We write the congruences

$$(31) \quad (\beta_1^2 + \beta_2^2 n)16d^2\sigma_2^2 - (g-f)(\gamma_5^2 + \rho\chi^2) - 2(f\rho - g)\chi\chi \equiv 0 \pmod{64d^2\sigma_2^2},$$

$$(32) \quad (2\beta_1\beta_2 + \beta_2^2)8d^2\sigma_2^2 - f(\gamma_5^2 + \rho\chi^2) - 2g\gamma_5\chi \equiv 0 \pmod{32d^2\sigma_2^2}.$$

Multiply (31) and (32) by g_1^2 , which is prime to $64d^2\sigma_2^2$ and write $\chi = -g_1\gamma_5$. The congruence (31) is then equivalent to

$$(\beta_1^2 + \beta_2^2 n)16g_1^2d^2\sigma_2^2 - \tau[(g_1-f_1)(X^2 + \rho g_1^2\gamma_5^2) - 2g_1(f_1\rho - g_1)\chi\chi] \equiv 0 \pmod{64d^2\sigma_2^2}$$

which by re-arranging terms and making use of the relation

$$g_1^2 = \sigma_2^2\sigma_1 + f_1^2\rho \quad \text{becomes}$$

$$(\beta_1^2 + \beta_2^2 n)16g_1^2d^2\sigma_2^2 - \tau(g_1-f_1)(X-f_1\rho\chi)^2 - \tau\sigma_2^2\chi[(g_1-f_1)\rho\chi + 2X] \equiv 0 \pmod{64d^2\sigma_2^2}.$$

If now we write as in §6

$$g_1^{\phi} = 1 + md\sigma_2$$

and write

$$\gamma_5 = -f_1\rho g_1^{\phi-1}\chi + \lambda d\sigma_2,$$

we obtain

$$\begin{aligned} X - \rho f_1\chi &= -g_1(-f_1\rho g_1^{\phi-1}\chi + \lambda d\sigma_2) - \rho f_1\chi \\ &= f_1\rho\chi(1 + md\sigma_2 - 1) - g_1\lambda d\sigma_2 \\ &= d\sigma_2(mf_1\rho\chi - g_1\lambda) = d\sigma_2 Y, \end{aligned}$$

and hence obtain

$$(33) \quad (\beta_1^2 + \beta_2^2 n)16g_1^2 - \tau(g_1-f_1)Y^2 - \tau\sigma_2^2\chi[(g_1+f_1)\rho\chi + 2d\sigma_2 Y] \equiv 0 \pmod{64}.$$

Likewise we have from (32)

$$(2\beta\beta_2 + \beta_2^2)8d^2\alpha_2^2g_1^2 - \tau f_1(X^2 + \rho g_1^2\chi^2) + 2\tau g_1^2X\chi \equiv 0 \pmod{32d^2\alpha_2^2}.$$

Again using $g^2 = \alpha_2^2\sigma_1 + f_1^2\rho$, re-arranging terms, and writing

$X - \rho f_1\chi = d\alpha_2Y$ as above we obtain

$$(2\beta\beta_2 + \beta_2^2)8d^2\alpha_2^2g_1^2 - \tau f_1d^2\alpha_2^2Y^2 + \tau\alpha_2^2\sigma_1(2d\alpha_2Y + f_1\rho\chi) \equiv 0 \pmod{32d^2\alpha_2^2}$$

from which

$$(34) \quad (2\beta\beta_2 + \beta_2^2)8g_1^2 - \tau f_1Y^2 + \tau\alpha_2\sigma_1(2d\alpha_2Y + f_1\rho\chi) \equiv 0 \pmod{32}$$

We will write $g_1 = f_1 + 2k$ and note the following relation when $\rho = 4n + 1$:

$$g_1^2 - f_1^2\rho = f_1^2 + 4f_1k + 4k^2 - f_1^2(4n+1) = 4[k(f_1+k) - f_1^2n] = \alpha_2^2\sigma_1.$$

Since σ_1 has no square factors, 4 divides α_2^2 . Hence if σ_1 is even, 2 must divide n , since either k or $f_1 + k$ is even. For convenience we display this table:

f, g	α_2	σ_1	$\tau\alpha_3$	τ	d	τ_2	n
$f \equiv g \equiv 1 \pmod{2}$	even	odd	odd	odd	odd	odd	$k(f_1+k) - f_1^2n \not\equiv 2 \pmod{4}$
$f \equiv g \equiv 2 \pmod{2}$	even	even	odd	even	even	odd	even
		odd			odd	even	$k(f_1+k) - f_1^2n \not\equiv 2 \pmod{4}$

Furthermore, the following discussion will be necessary for later development:

Let q be an odd integer, g_1 odd and prime to q , $e \geq 1$.

Then

$$g_1\phi(2^e q)_{-1} = [g_1\phi(q)]2^{e-1}_{-1}$$

$$= \{(g_1\phi(q))2^{e-2}_{+1}\} \{(g_1\phi(q))2^{e-3}_{+1}\} \dots \{(g_1\phi(q))2^{e-e}_{+1}\} \{g_1\phi(q)_{-1}\}$$

Evidently all the factors in the product on the right are divisible by 2, and either the last or the next to the last is divisible by 4. Hence, omitting the case $e = 1, q = 1$, the product is divisible by 2^{e+1} . In view of this fact and of our transformation in Section 2 which insured $\sigma_2 > 4$ for the case $f \equiv g \equiv 2 \pmod{4}$, σ_1 odd, we see that the m defined in Section 6 is even for $g \equiv f \equiv 2 \pmod{4}$.

We will consider now case I, $f \equiv g \equiv 1 \pmod{2}$, with σ_3 odd. The congruence (33) may be written

$$(35) \quad (\beta^2 + \beta_1^2 n) 8g_1^2 - k\tau Y^2 - rt\tau_2\sigma_3\chi [(f_1+k)\rho\chi + d\alpha_2 Y] \equiv 0 \pmod{32}.$$

From (35) either Y or χ is even, since $k \not\equiv k + f_1 \pmod{2}$. From (34) $Y \equiv \chi \pmod{2}$. Hence $\chi \equiv Y \equiv \lambda \equiv 0 \pmod{2}$. Using the notation

$$Y' = mf_1\rho\chi_0 - g_1\lambda_1, \quad \chi = 2\chi_0, \quad \lambda = 2\lambda_1$$

we have

$$(36) \quad (\beta^2 + \beta_1^2 n) 2g_1^2 - k\tau Y'^2 - rt\tau_2\sigma_3\chi_0 [(f_1+k)\rho\chi_0 + d\alpha_2 Y'] \equiv 0 \pmod{8},$$

$$(37) \quad (2\beta\beta_2 + \beta_2^2) 2g_1^2 - \tau f_1 Y'^2 + rt\tau_2\sigma_3\chi_0 [f_1\rho\chi_0 + 2d\alpha_2 Y'] \equiv 0 \pmod{8}.$$

Exactly as before we have $Y' \equiv \chi_0 \equiv \lambda_1 \equiv 0 \pmod{2}$ and it follows from (37) that $\beta_2 \equiv 0 \pmod{2}$ and hence from (36) that $\beta_1 \equiv 0 \pmod{2}$. Finally $Y'' \equiv \chi_0 \equiv 0 \pmod{2}$, where $Y'' = mf_1\rho\chi_0 - g_1\lambda_2$, $\chi_0 = 2\chi_0$, $\lambda_1 = 2\lambda_2$. Hence in this case our integers have the form

$$J = \beta_3 + \beta_4 P + \lambda_3 i + \chi_2 w.$$

Next we consider case II in which $f \equiv g \equiv 2 \pmod{4}$ and σ_1 is even. We start again with the congruences (34) and (35).

Clearly as displayed in the table above τ_2 is odd and

$d \equiv n \equiv 0 \pmod{2}$. Then from (34) $\chi \equiv 0 \pmod{2}$ and hence, since $\tau \equiv 2 \pmod{4}$, $Y \equiv 0 \pmod{2}$, and therefore $\lambda \equiv 0 \pmod{2}$. Hence we have again (36) and (37). From (37) $\gamma_0 \equiv 0 \pmod{2}$ and hence $\beta \equiv Y' \equiv \lambda, \pmod{2}$. Writing $\tau = 2\tau'$ and dropping the factor $\tau_2\sigma_2$ from the last term and g_1^2 from the first term we have

$$(38) \quad (\beta^2 + \lambda^2 n) - k\tau'\lambda^2 - 2(f_1+k)\gamma_0 \equiv 0 \pmod{4},$$

$$(39) \quad (2\beta\lambda + \lambda^2) - \tau'f_1\lambda^2 + 2f_1\gamma_0^2 \equiv 0 \pmod{4}.$$

If we adopt the notation $f = 2f'$ as in §4 and if $f' \equiv 1 \pmod{4}$ our congruences are equivalent to

$$(40) \quad \beta^2 + \lambda^2(n - k\tau') - 2(1+k)\beta\lambda, \equiv 0 \pmod{4},$$

$$(41) \quad \beta, \lambda + \gamma_0^2 \equiv 0 \pmod{2}$$

which were obtained by solving (39) for γ_0^2 and substituting in (38). Then, recalling that n is even,

If $n - k\tau' \equiv 0 \pmod{4}$, the solutions are $\beta \equiv \beta_2 \equiv \lambda \equiv \gamma_0 \equiv 0 \pmod{2}$ and $\beta_1 \equiv 0, \beta_2 \equiv \lambda \equiv 1, \gamma_0 \equiv 0 \pmod{2}$.

If $n - k\tau' \equiv 2$ or $1 \pmod{4}$, the solution is $\beta \equiv \beta_2 \equiv \lambda \equiv \gamma_0 \equiv 0 \pmod{2}$.

If $n - k\tau' \equiv 3 \pmod{4}$, the solutions are $\beta \equiv \beta_2 \equiv \lambda \equiv \gamma_0 \equiv 0$ or $1 \pmod{2}$.

Similarly if $f' \equiv 3 \pmod{4}$ our congruences are equivalent to

$$\beta^2 + \lambda^2 [n - k\tau' - 2(1+k)] + 2(f_1+k)\beta\lambda \equiv 0 \pmod{4},$$

$$\beta, \lambda - \lambda^2 + \gamma_0^2 \equiv 0 \pmod{2}.$$

If $n - k\tau' - 2(1+k) \equiv 0 \pmod{4}$ the solutions are $\beta_1 \equiv 0, \beta_2 \equiv \lambda \equiv \gamma_0 \equiv 0$ or $1 \pmod{2}$.

If $n - k\tau' - 2(1+k) \equiv 2$ or $1 \pmod{4}$ the solution is $\beta_1 \equiv \beta_2 \equiv \lambda \equiv \gamma_0 \equiv 0 \pmod{2}$.

If $n - k\tau' - 2(1+k) \equiv 3 \pmod{4}$ the solutions are
 $\beta_1 \equiv \beta_2 \equiv \lambda_1 \equiv 1$ or 0 , $\gamma_0 \equiv 0 \pmod{2}$.

In cases III and IV τ_2 is even and $\sigma\sigma_2 rtd \equiv 1 \pmod{2}$. Hence from (35) either Y or $\lambda \equiv 0 \pmod{2}$ and from (34) $Y \equiv \lambda \pmod{2}$. Hence $\lambda \equiv Y \equiv 0 \pmod{2}$. Hence (34) and (35) become

$$(42) \quad (\beta_1^2 + \beta_2^2 n) - k\tau'Y'^2 - rt\tau_2'\alpha_2\gamma_0[(f_1+k)\gamma_0 + d\sigma_2Y] \equiv 0 \pmod{4},$$

$$(43) \quad (2\beta_1\beta_2 + \beta_2^2) - \tau'f_1Y'^2 + rt\tau_2'\alpha_2\gamma_0^2 f_1 \equiv 0 \pmod{4},$$

where $2\tau_2' = \tau_2$. Hence in case III for which $\sigma \equiv 1$, $f' \equiv 1 \pmod{4}$ we obtain, if we replace γ_0^2 in (42) by its value from (43), the congruences

$$\begin{aligned} \beta_1^2 + \beta_2^2(n+k\tau'+1) + Y'^2(2k-1) + 2\beta_1\beta_2(k+1) + \alpha_2Y'\gamma_0 &\equiv 0 \pmod{4}, \\ \gamma_0^2 &\equiv Y'^2 - 2\beta_1\beta_2 - \beta_2^2 \pmod{4}. \end{aligned}$$

It should be noted that in (42) and (43) $rt\tau_2'\alpha_2f_1$ may be multiplied by $d^2 \equiv 1 \pmod{4}$, obtaining $\tau'f_1 = f'$. Furthermore, n even implies $\lambda \equiv Y' \pmod{2}$.

If $(n+k\tau'+1) \equiv 0 \pmod{2}$, the solution is $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0 \pmod{2}$.

If $1 \pmod{2}$, the solutions are $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0$;
 $\beta_1 \equiv \beta_2 \equiv \gamma_0 \equiv 1$, $Y' \equiv 0$; $\beta_1 \equiv \gamma_0 \equiv 0$, $\beta_2 \equiv Y' \equiv 1$; $\beta_2 \equiv Y' \equiv \gamma_0 \equiv 1$,
 $\beta_2 \equiv 0 \pmod{2}$.

In case IVa in which $\sigma \equiv 3$, $f' \equiv 1 \pmod{4}$ the congruences (42) and (43) become

$$\begin{aligned} \beta_1^2 + \beta_2^2(n+k\tau'+1) - Y'^2(2k+1) + 2\beta_1\beta_2(k+1) + \sigma_2Y'\gamma_0 &\equiv 0 \pmod{4}, \\ \gamma_0^2 &\equiv 2\beta_1\beta_2 + \beta_2^2 - Y'^2 \pmod{4} \end{aligned}$$

¹It is understood of course that the conditions $f' \equiv 1$, $\sigma \equiv 1 \pmod{4}$ and hence $k(f_1+k)-f_1^2n \not\equiv 2 \pmod{4}$ are to be satisfied first. In this case this precludes the possibility of $n \equiv 1 \pmod{2}$ as a solution for $(n+k\tau'+1) \equiv 1 \pmod{4}$ and $n \equiv 0 \pmod{2}$ for $(n+k\tau'+1) \equiv 3 \pmod{4}$. It should also be noted that n even implies $\sigma_2 \equiv 0 \pmod{4}$, n odd implies $\sigma_2 \equiv 2 \pmod{4}$.

If $n+k\tau'+1 \equiv 0 \pmod{4}$ the solutions are $\beta_1 \equiv Y' \equiv 0$, $\beta_2 \equiv \gamma_0 \pmod{2}$.

If $n+k\tau'+1 \equiv 2 \pmod{4}$ or if $n+k\tau'+1 \equiv 1 \pmod{4}$ with k odd, the solution is $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0 \pmod{2}$.

If $n+k\tau'+1 \equiv 1 \pmod{4}$ with k even the solutions are $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0$; $\beta_1 \equiv \beta_2 \equiv 0$, $\beta_2 \equiv Y' \equiv 1 \pmod{2}$.

The case $n+k\tau'+1 \equiv 3 \pmod{4}$ does not appear in this case.

Finally in case IVb in which $\sigma_f \equiv 3$, $f' \equiv 3 \pmod{4}$ the congruences (42) and (43) become

$$\begin{aligned} \beta_1^2 + \beta_2^2(n-k\tau'+1) + Y'^2(2k+1) - 2\beta_1\beta_2(k+1) + \alpha_2\gamma_0Y' &\equiv 0 \pmod{4}, \\ 2\beta_1\beta_2 + \beta_2^2 + Y'^2 + \gamma_0^2 &\equiv 0 \pmod{4}. \end{aligned}$$

If $n-k\tau'+1 \equiv 0 \pmod{4}$ the solutions are $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0$ and $\beta_1 \equiv \beta_2 \equiv Y' \equiv 1$, $\gamma_0 \equiv 0 \pmod{2}$.

If $n-k\tau'+1 \equiv 2 \pmod{4}$ or if $n-k\tau'+1 \equiv 1 \pmod{4}$ with k odd, the solution is $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0 \pmod{2}$.

If $n-k\tau'+1 \equiv 1 \pmod{4}$ with k even the solutions are $\beta_1 \equiv \beta_2 \equiv Y' \equiv \gamma_0 \equiv 0$ and $\beta_1 \equiv \beta_2 \equiv \gamma_0 \equiv 1$, $Y' \equiv 0 \pmod{2}$.

Again the case $n-k\tau'+1 \equiv 3 \pmod{4}$ is impossible.

As in Sections 7 and 8 the solutions of the congruences show the form the integers must take in the various cases. The bases can then be computed and the results checked as before, attention being paid to the fact that the basis for $R(u)$ is $1, P$ where $P = (u+1)/2$. The results may be summarized in the following final theorem.

THEOREM 10. Let $R(1)$ be a G_8 field of Theorem 8 with $\rho = 4n+1$. Let α , α_2 , and w be defined as in §6 and k, τ' , and γ_0 as in §9. Finally let $2w_1 = w$, $2i_1 = 1$, where i_1, w_1 are integers of $R(1)$ in the cases where they appear below. Then the values of the parameters which give rise to non-equivalent fields are

(1) $f \equiv g \equiv 1 \pmod{2}$, σ odd, in which case $(1, P, i, w)$ form a basis for the integers of $R(i)$;

(2) $f \equiv 2 \pmod{8}$, $g \equiv 2 \pmod{4}$, σ even, in which case $(1, P, [P+i_1]/2, w)$ form a basis if $n-k\tau' \equiv 0 \pmod{4}$, $(1, P, i_1, w)$ form a basis if $n-k\tau' \equiv 2$ or $1 \pmod{4}$, and $(1, P, [1+P+w+i_1]/2, w)$ form a basis if $n-k\tau' \equiv 3 \pmod{4}$;

(3) $f \equiv 6 \pmod{8}$, $g \equiv 2 \pmod{4}$, σ even, in which case $(1, P, [P+i_1+w]/2, w)$ form a basis if $n-k\tau'-2(1+k) \equiv 0 \pmod{4}$, $(1, P, i_1, w)$ form a basis if $n-k\tau'-2(1+k) \equiv 2$ or $1 \pmod{4}$, and $(1, P, [1+P+i_1]/2, w)$ form a basis if $n-k\tau'-2(1+k) \equiv 3 \pmod{4}$;

(4) $f \equiv 2 \pmod{8}$, $g \equiv 2 \pmod{4}$, $\sigma \equiv 1 \pmod{4}$, in which case $(1, P, i_1, w_1)$ form a basis if $(n+k\tau'+1) \equiv 0 \pmod{2}$, and $(1, P, [P+i_1]/2, [1+i_1+w_1]/2)$ form a basis if $(n+k\tau'+1) \equiv 1 \pmod{2}$;

(5) $f \equiv 2 \pmod{8}$, $g \equiv 2 \pmod{4}$, $\sigma \equiv 3 \pmod{4}$, $\sigma_2 > 2$, in which case $(1, P, i_1, [P+w_1]/2)$ form a basis if $(n+k\tau'+1) \equiv 0 \pmod{4}$, $(1, P, i_1, w_1)$ form a basis if $(n+k\tau'+1) \equiv 2 \pmod{4}$ or $\equiv 1 \pmod{4}$, k odd, and $(1, P, [P+i_1]/2, w_1)$ form a basis if $(n+k\tau'+1) \equiv 1 \pmod{4}$, k even;

(6) $f \equiv 6 \pmod{8}$, $g \equiv 2 \pmod{4}$, $\sigma \equiv 3 \pmod{4}$, $\sigma_2 > 2$, in which case $(1, P, [1+P+i_1]/2, w_1)$ form a basis if $n-k\tau'+1 \equiv 0 \pmod{4}$, $(1, P, i_1, w_1)$ form a basis if $n-k\tau'+1 \equiv 2 \pmod{4}$ or $\equiv 1 \pmod{4}$, k odd, and $(1, P, i_1, [1+P+w_1]/2)$ form a basis if $n-k\tau'+1 \equiv 1 \pmod{4}$, k even.

VITA

Antoinette Marie Killen was born in Chicago, Illinois, on November 23, 1904. She received her early education in the Chicago public schools, graduating from the Nicholas Senn High School in June, 1923. She entered the University of Chicago the following autumn, receiving the degree of Bachelor of Science in June, 1926, and the degree of Master of Science in June, 1930. She continued her studies at the University, while acting as Assistant Secretary in the Department of Mathematics, doing graduate work under Professors Albert, Barnard, Bartky, Bliss, Dickson, Graves, Lane, Logsdon, Lunn, and MacMillan.

The author takes this opportunity to acknowledge her gratitude to all the members of this Department, and in particular to Professor Albert whose paper on "The integers of normal quartic fields" furnished the inspiration for this dissertation, and under whose constant guidance and assistance it was written.

